

Alerta de seguridad informática	8FFR-00011-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Agosto de 2019
Última revisión	09 de Agosto de 2019

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigaciones propias del equipo CSIRT. La información contenida en los informes o comunicados está afectada a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnica de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado un dominio fraudulento que no pertenecía al Banco de Chile, el que sospecha sería utilizado para suplantar el sitio web oficial del **BANCODECHILE.CL** con el objetivo de realizar algún fraude bancario.

El CSIRT informó oportunamente a la entidad bancaria con el objetivo de desechar cualquier tipo de relación de propiedad u otra con el sitio sospechoso, así como para coordinar una respuesta adecuada para contener el incidente.

Indicadores de Compromisos

Dominios

3barcochile-cl[.]xyz[.]
bancochile[.]xyz[.]
barcochile-cl[.]xyz[.]
barcochile-com-cl[.]xyz[.]
Xnbncochile52a[.]xyz[.]

Recomendaciones

- Evitar acceder a los sitios que provienen de los dominios anteriormente indicados e informar a los usuarios sobre la existencia del sitio, para que no ser víctimas del fraude.
- Ser precavidos frente a páginas fraudulentas, provienen de los dominios Informados.
- Bloquear en los proxy o sistemas de control de contenido
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing